



Séminaire de l'Association Europe Finances Régulations
Souveraineté numérique : quels enjeux pour l'Europe ?

Paris, 15 octobre 2026

**Innovation, sécurité et souveraineté technologique,
des impératifs à concilier**

Discours de Denis Beau
Premier sous-gouverneur de la Banque de France
et Président désigné de l'ACPR

Mesdames et messieurs,

Je voudrais d'abord remercier l'Association Europe-Finances-Régulations qui m'a aimablement invité à ouvrir les débats de ce séminaire consacré à la souveraineté numérique et à la résilience opérationnelle du secteur financier, que je suis très heureux d'accueillir ici, à la Banque de France.

Le secteur financier est aujourd'hui confronté à un double impératif : développer son offre de services numériques tout en garantissant la sécurité de ses opérations.

Pour y parvenir, **la solution la plus évidente est bien souvent de recourir aux *hyperscalers***, qui proposent des infrastructures et des services très performants, en particulier en matière de cloud et d'IA, tout en offrant des garanties de sécurité à l'état de l'art. Ce choix **expose cependant à un nouveau risque : la dépendance numérique**. Celle-ci est potentiellement coûteuse sur le long terme : une étude mandatée par le CIGREF avance le chiffre de 264 milliards d'euros dépensés chaque année par les Européens en logiciels et services cloud américains¹. Elle est aussi opérationnellement dangereuse, comme le montrent les discussions autour du scénario d'un « *kill switch* » sur les services numériques américains.

Cette situation illustre la difficulté des choix technologiques auxquels sont aujourd'hui confrontés les acteurs financiers. **Dès lors, l'enjeu est de faire en sorte qu'innovation, sécurité et souveraineté ne constituent pas des injonctions contradictoires**. Dans ce contexte, je voudrais d'abord revenir sur les risques qu'une situation de dépendance ferait peser sur le secteur financier (I), avant de discuter des réponses opérationnelles que les acteurs financiers et les autorités publiques peuvent chacun déployer (II).

*

I/ Les risques de sécurité et de souveraineté sont liés à un même problème de maîtrise : celui des infrastructures numériques critiques. En donnant « les clés du véhicule » à quelques prestataires incontournables sur lesquels elles n'ont que peu de levier, les entités financières se mettent dans une situation de vulnérabilité, **pour au moins trois raisons**.

D'abord, la concentration des fournisseurs constitue en elle-même un nouveau risque opérationnel, et peut même concerner les solutions de cybersécurité : ainsi, pendant l'incident CrowdStrike de juillet 2024, une mise à jour défectueuse a mis en panne 8,5 millions d'ordinateurs à travers le monde. **Ensuite, la dépendance réduit la capacité de maîtrise du risque opérationnel** – dont le risque cyber – par les établissements. À force de confier certaines activités à des tiers, **les établissements peuvent perdre la capacité de les réaliser eux-mêmes et, surtout, d'en apprécier pleinement la qualité**. Cette perte d'expertise rend ainsi plus difficile le contrôle effectif des prestataires informatiques. **Enfin, en externalisant certains services critiques, les établissements s'exposent à un phénomène d'« enfermement »** par les

fournisseurs (**vendor lock-in**), qui peuvent se matérialiser très concrètement par des augmentations substantielles de coûts une fois la dépendance créée, ou encore, ce qui revient au même, par l'obligation de payer des fonctionnalités superflues (pratique du *bundling*).

Éviter d'être exposé à ces risques de dépendance technologique n'est pas simple. Le cas des **modèles d'IA de pointe** fournit un exemple particulièrement éclairant. D'une part, il est de plus en plus clair que ces modèles vont constituer un outil incontournable pour la cybersécurité car, à côté des capacités offensives qu'ils peuvent malheureusement offrir aux attaquants, ils apportent de nouvelles possibilités aux équipes de sécurité, tant pour l'identification de vulnérabilités que pour la génération automatisée de correctifs. **Mais tirer pleinement parti de ces solutions suppose souvent de leur accorder un accès très étendu au système d'information de l'établissement, ce qui crée en retour de nouveaux risques** : risque de compromission, mais aussi risque de transfert du capital informationnel du secteur financier vers quelques grands fournisseurs technologiques extra-européens.

II/ Comment concilier alors innovation, sécurité et maîtrise du risque de dépendance technologique ? Sans prétendre épuiser un sujet aussi vaste, je voudrais évoquer quelques leviers d'action à la disposition des acteurs financiers, ainsi que le rôle essentiel que les autorités publiques ont à jouer.

Les entités, d'abord, doivent renforcer la prise en compte des dépendances dans leur analyse du risque opérationnel en réalisant un **inventaire systématique des dépendances critiques** couvrant l'ensemble de leurs actifs informatiques – postes de travail, réseaux, matériels, logiciels, services cloud, équipements de sécurité etc. Bien que complexe, cet exercice est indispensable pour disposer d'une vision complète de l'exposition au risque. Des indicateurs de référence, tels que l'indice de résilience numérique (IRN), développé par un consortium d'acteurs publics, d'entreprises et d'experts du numérique, peuvent utilement contribuer à cette évaluationⁱⁱ.

L'identification des dépendances doit ensuite permettre aux entités d'élaborer des stratégies de résilience opérationnelle qui soient compatibles avec leur maîtrise de leurs infrastructures technologiques, leurs données et leurs compétences numériques critiques, en mettant par exemple en place des stratégies « multi-cloud », des stratégies de « cloud hybride », ou encore en préparant des options de sortie en assurant la portabilité des données et des applications. Le recours à des **solutions open source** constitue également une piste prometteuse pour limiter les dépendances à des technologies propriétaires extra-européennes.

Évidemment, face à des enjeux qui dépassent le périmètre de chaque établissement, **les pouvoirs publics ont aussi leur rôle à jouer**. Je voudrais souligner en premier lieu que les **réglementations européennes**, telles que le RGPD ou le règlement IA, en promouvant des valeurs européennes fondamentales, **concourent puissamment à l’affirmation de notre souveraineté**. Ne cédon pas à la tentation de les considérer comme des freins à l’innovation, par une inversion dangereuse de la hiérarchie entre la fin et les moyens.

Encore faut-il que cette souveraineté normative s’appuie sur des capacités technologiques réelles. Le « paquet de souveraineté technologique » proposé par la Commission Européenne, qui intègre notamment le *Cloud & AI Development Act (CADA)*^{iv}, constitue à cet égard une nouvelle étape importante. D’autres intervenants plus qualifiés y reviendront par la suite, mais ce texte vise à faciliter le déploiement du cloud et de l’IA dans l’UE ; il propose en particulier une **classification unique** pour évaluer le niveau de souveraineté d’un service cloud^v. Le paquet comprend aussi une Stratégie *open source* visant à **assurer un accès continu aux briques logicielles les plus critiques**.

Au-delà de la définition des règles, les autorités publiques ont également un rôle essentiel à jouer dans leur mise en œuvre concrète. Cela passe d’abord par la coopération étroite entre nos différentes institutions de contrôle, indispensable à la fois pour partager l’information et pour assurer une coordination efficace lorsque nos champs de compétence se rejoignent, voire se chevauchent. **La Banque de France et l’ACPR ont ainsi renouvelé leur accord de coopération avec l’ANSSI**, en juillet dernierⁱⁱⁱ, afin de poursuivre le développement de nos synergies opérationnelles et de les adapter au nouveau cadre issu des évolutions réglementaires.

Les autorités financières, quant à elles, peuvent jouer au moins deux rôles complémentaires. En premier lieu, **un rôle de vigie** au travers de leur mission de surveillance. La mise en œuvre du **règlement DORA** nous a amenés aussi à monter en puissance sur plusieurs sujets, comme les tests de résilience numérique ou le suivi des incidents majeurs notifiés par le secteur. L’exercice efficace de cette mission suppose une **veille constante sur les risques numériques et la menace cyber**. C’est ainsi que les développements de l’**IA de pointe** nous ont conduits à élaborer un plan d’action spécifique, détaillé dans une **communication envoyée par l’ACPR aux fédérations professionnelles en juin dernier**. Celui-ci met l’accent sur deux priorités : d’une part, la mise en œuvre de mesures d’hygiène cyber fondamentales et, d’autre part, le déploiement plus rapide de correctifs de sécurité afin de répondre à l’accélération du rythme d’exploitation des vulnérabilités par les acteurs malveillants.

De plus, en soumettant les **prestataires informatiques critiques** (*Critical Third-Party Providers* ou CTPPs) à **un dispositif européen de surveillance coordonnée**, DORA permet aux superviseurs financiers de mieux évaluer les risques de concentration, de dépendance et de

verrouillage technologique. À terme, cela leur permettra de mieux articuler les objectifs de sécurité opérationnelle et de souveraineté numérique, de promouvoir des pratiques adaptées et d'adapter leur action aux évolutions rapides de l'environnement technologique.

En second lieu, nous pouvons exercer un **rôle d'entraînement par les choix technologiques que nous effectuons pour nos besoins propres**, choix qui sont susceptibles d'influencer les décisions du secteur financier. De fait, la **Banque de France** est elle-même confrontée aux arbitrages difficiles que j'évoquais précédemment, notamment dans ses missions de banque centrale et d'opérateur d'infrastructures de marché. Pour y répondre, elle a décidé de se doter d'une **doctrine de souveraineté numérique**, qui alimente directement notre feuille de route stratégique 2028 et la gestion de nos projets informatiques. **Cette doctrine peut se résumer en une phrase : maîtriser nos données, nos infrastructures, et les compétences pour les opérer.**

Pour illustrer cette doctrine, je voudrais pour finir évoquer **deux projets en cours**. Premièrement, l'arrivée prochaine de **solutions Mistral AI hébergées en cloud souverain**, pour un usage quotidien par nos agents, mais aussi pour la protection de nos systèmes d'information. Et, deuxièmement, la construction d'une **solution de virtualisation de notre cloud privé** basée sur des technologies *open source*, qui doit nous permettre d'optimiser nos ressources informatiques sans dépendre d'outils propriétaires. Nous étudions en outre, au sein de l'Eurosystème, les leviers d'action collectifs pour réduire les risques majeurs vis-à-vis des fournisseurs.

*

Vous l'aurez compris, ma conviction est que pour bien articuler innovation, sécurité et souveraineté, il est essentiel d'assurer la maîtrise opérationnelle de nos infrastructures numériques avec une stratégie claire et cohérente. Les évolutions législatives récentes et à venir visent précisément à encourager le secteur financier à intégrer pleinement ces enjeux dans ses décisions, et à élargir l'éventail de solutions européennes disponibles en favorisant l'émergence et le développement d'offres souveraines. Je forme donc le vœu que les débats de ce matin contribuent utilement à cette réflexion collective, et je vous souhaite un excellent séminaire.

ⁱ [Étude CIGREF](#), 2025. Chiffres extrapolés à partir des dépenses de 6 grandes entreprises « témoin ».

ⁱⁱ [aDRI - Indice de Résilience Numérique](#)

ⁱⁱⁱ [L'ANSSI, l'ACPR et la Banque de France signent un accord et renforcent leur coopération en matière de sécurité des systèmes d'information | Banque de France](#)

^{iv} [Communication sur la souveraineté technologique européenne, accompagnée d'une stratégie de l'UE en matière d'open source | Bâtir l'avenir numérique de l'Europe](#)

^v [Règlement sur le développement de l'informatique en nuage et de l'IA | Bâtir l'avenir numérique de l'Europe](#)